

Intelegjenca Kërcënuese

Burimet e Informacionit

Komunitetet e Inteligjencës së Rrjetit

- Organizatat e inteligjencës kërcënuese si CERT, SANS dhe MITER ofrojnë informacione të hollësishme mbi kërcënimet që janë jetike për praktikat e sigurisë kibernetike.



Burimet e Informacionit

Raportet e Cisco Cybersecurity

- Cisco ofron Raportin e Sigurisë së Kibernetikës çdo vit, i cili siguron një përditësim mbi gjendjen e gatishmërisë së sigurisë, analizën e ekspertëve të dobësive më të mira, faktorët pas shpërthimit të sulmeve duke përdorur adware dhe spam, dhe më shumë.



Burimet e Informacionit

Bloget e Sigurisë dhe Podcasts

- Bloget dhe podcasts e sigurisë ndihmojnë profesionistët e sigurisë kibernetike të kuptojnë dhe zbusin kërcënimet në zhvillim



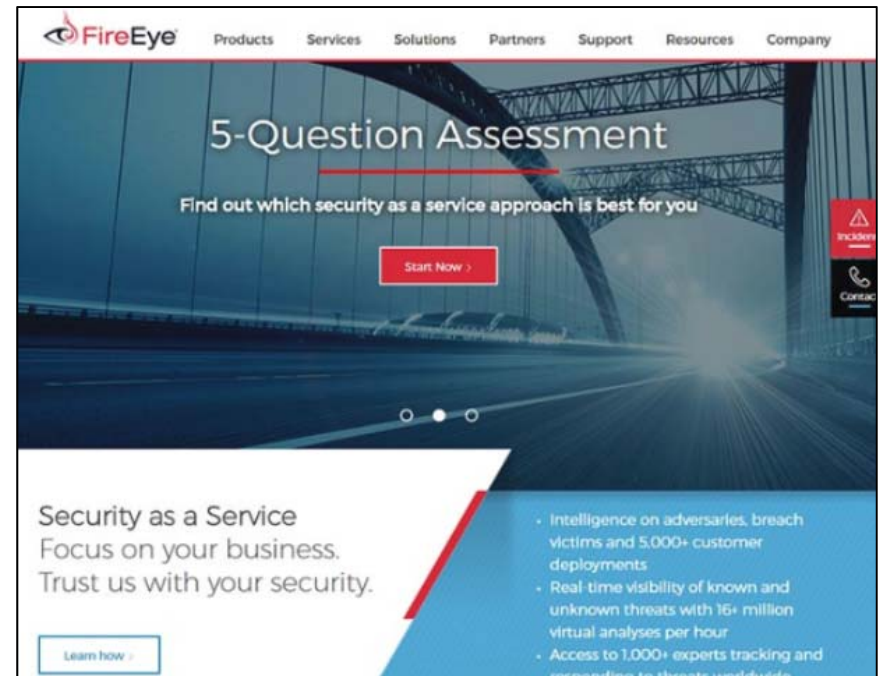
Shërbimet e inteligjencës kërcënuese Cisco Talos

- Shërbimet e inteligjencës kërcënuese lejojnë shkëmbimin e informacionit të kërcënimeve të tilla si dobësitë, treguesit e kompromisit (IOC), dhe teknikat e zbutjes dhe zbulimit.
- Cisco Talos mbledh informacione për kërcënimet aktive, ekzistuese dhe ato në zhvillim. Talos pastaj u siguron abonentëve të saj mbrojtje të plotë kundër këtyre sulmeve dhe malware.



Shërbimet e inteligjencës kërcënuese FireEye

- FireEye është një kompani tjetër sigurie që ofron shërbime për të ndihmuar ndërmarrjet të sigurojnë rrjetet e tyre.
- FireEye ofron informacion të kërcënimit në rritje dhe raporte të inteligjencës së kërcënimit.



Shërbimet e inteligjencës kërcënuese Ndarja e treguesve të automatizuar

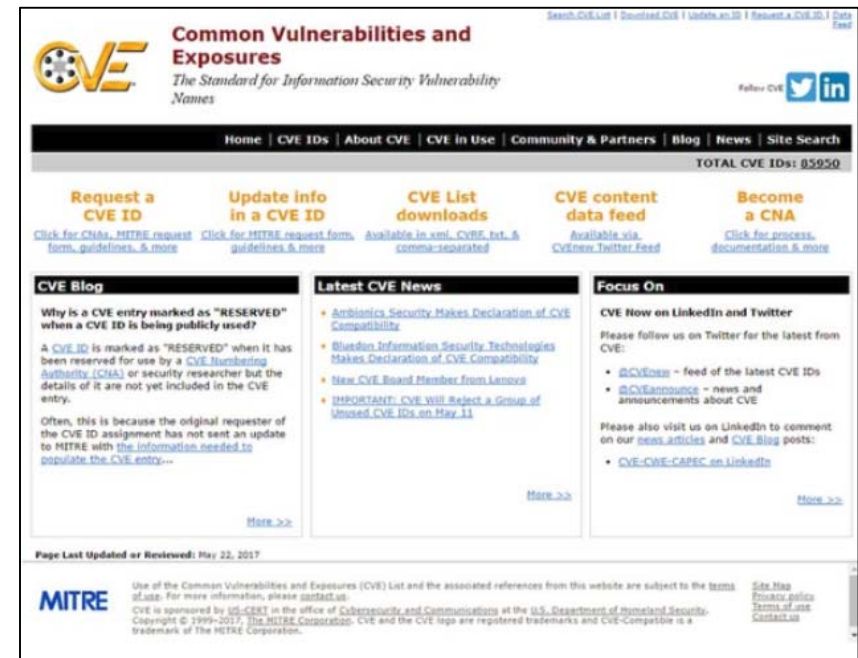
- Automated Indicator Sharing (AIS) është një program që lejon qeverinë federale të SHBA-së dhe sektorin privat të ndajnë treguesit e kërcënimeve.
- AIS krijon një ekosistem ku, sapo të njihet një kërcënim, ajo ndahet menjëherë me komunitetin.



Shërbimet e inteligjencës kërcënuese

Baza e të Dhënave të Cenueshmërisë dhe Ekspozimeve të Përbashkëta

- Common Vulnerabilities and Exposures (CVE) është një bazë të dhënash për dobësitë që përdor një skemë të standardizuar të emërimit për të lehtësuar ndarjen e inteligjencës së kërcënimit.



The screenshot shows the homepage of the Common Vulnerabilities and Exposures (CVE) website. The header features the CVE logo, the title "Common Vulnerabilities and Exposures", and the tagline "The Standard for Information Security Vulnerability Names". Navigation links include Home, CVE IDs, About CVE, CVE in Use, Community & Partners, Blog, News, and Site Search. A search bar is located in the top right corner. The main content area is divided into several sections: "Request a CVE ID", "Update info in a CVE ID", "CVE List downloads", "CVE content data feed", and "Become a CNA". Below these are three columns: "CVE Blog" with an article about "RESERVED" entries, "Latest CVE News" with a list of recent updates, and "Focus On" with information about CVE on LinkedIn and Twitter. The footer contains the MITRE logo, a disclaimer about the use of the CVE list, and links to the privacy policy and terms of use.

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

Home | CVE IDs | About CVE | CVE in Use | Community & Partners | Blog | News | Site Search

TOTAL CVE IDs: 85950

Request a CVE ID
[Click for CHAs, MITRE request form, guidelines, & more](#)

Update info in a CVE ID
[Click for MITRE request form, guidelines, & more](#)

CVE List downloads
[Available in xml, CVE, txt, & comma-separated](#)

CVE content data feed
[Available via CVEnew Twitter Feed](#)

Become a CNA
[Click for process, documentation, & more](#)

CVE Blog
Why is a CVE entry marked as "RESERVED" when a CVE ID is being publicly used?
A CVE ID is marked as "RESERVED" when it has been reserved for use by a [CVE Numbering Authority \(CNA\)](#) or security researcher but the details of it are not yet included in the CVE entry.
Often, this is because the original requester of the CVE ID assignment has not sent an update to MITRE with the [information needed to populate the CVE entry](#)...
[More >>](#)

Latest CVE News

- [Ambionics Security Makes Declaration of CVE Compatibility](#)
- [Bluelion Information Security Technologies Makes Declaration of CVE Compatibility](#)
- [New CVE Board Member from Lenovo](#)
- [IMPORTANT: CVE Will Reject a Group of Unused CVE IDs on May 11](#)

[More >>](#)

Focus On
CVE Now on LinkedIn and Twitter
Please follow us on Twitter for the latest from CVE:

- [@CVEnew](#) - feed of the latest CVE IDs
- [@CVEannounce](#) - news and announcements about CVE

Please also visit us on LinkedIn to comment on our [news articles](#) and [CVE Blog](#) posts:

- [CVE-CWE-CAPEC on LinkedIn](#)

[More >>](#)

Page Last Updated or Reviewed: May 22, 2017


MITRE
Use of the Common Vulnerabilities and Exposures (CVE) List and the associated references from this website are subject to the [terms of use](#). For more information, please [contact us](#).
CVE is sponsored by [US-CERT](#) in the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.
Copyright © 1999-2017 The MITRE Corporation. CVE and the CVE logo are registered trademarks and CVE-Compliant is a trademark of The MITRE Corporation.

[Site Map](#)
[Privacy policy](#)
[Terms of use](#)
[Contact us](#)

Shërbimet e inteligjencës kërcënuese

Intelegjenca Kërcënuese dhe Standardet e Komunikimit

- Standardet e Inteligjencës Kërcënuese (CTI) si STIX dhe TAXII lehtësojnë shkëmbimin e informacionit të kërcënimit duke specifikuar strukturat e të dhënave dhe protokollet e komunikimit:
 - Shprehja e informacionit të kërcënimit të strukturuar (STIX) - specifikimet për shkëmbimin e informacionit të kërcënimit kibernetik në mes të organizatave.
 - Shkëmbimi i automatizuar i informacionit të treguesit (TAXII) - specifikim për një protokoll shtresash aplikimi që lejon komunikimin e CTI mbi HTTPS. TAXII është projektuar për të mbështetur STIX.



A structured language for cyber threat intelligence


[Read the Latest Specification! \(2.0 CSD 1\)](#)

[STIX 2.0 Public Review - Frequently Asked Questions](#)


Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.



STIX Relationship Diagram with Sighting




A transport mechanism for sharing cyber threat intelligence

[Read the Latest Specification! \(Draft 2\)](#)

Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.

TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.

TAXII is specifically designed to support the exchange of CTI represented in STIX.



TAXII Collections and Channels

Links:

- [Archive of TAXII 1.x](#)

Përmbledhje

- Rreziku i sigurisë në internet përbëhet nga asetet, dobësitë dhe kërcënimet.
- Asetet përbëjnë sipërfaqen e sulmit që kërcënojnë aktorët mund të synojnë.
- Rreziqet përfshijnë çdo dobësi të shfrytëzueshme në një sistem ose në dizajnin e tij.
- Kërcënimet lehtësohen më mirë duke përdorur një qasje mbrojtëse në thellësi.
- Analogjia e qepëve të sigurisë ilustron një qasje të shtresuar ndaj sigurisë.
- Analogjia e artichokës së sigurisë më mirë përfaqëson rrjetet e sotme.
- Politikat e biznesit janë udhëzimet e zhvilluara nga një organizatë për të qeverisur veprimet e saj dhe veprimet e punonjësve të saj.
- Një politikë sigurie identifikon një sërë objektivash të sigurisë për një kompani, përcakton rregullat e sjelljes për përdoruesit dhe administratorët dhe përcakton kërkesat e sistemit.

Përmbledhje

- Një politikë BYOD, e cila u mundëson punonjësve të përdorin pajisjet e tyre mobile për të pasur akses në burimet e kompanisë, rregullon cilat punonjës u lejohet të kenë qasje në burimet që përdorin pajisjet e tyre personale.
- Të gjitha organizatat duhet të jenë në përputhje me rregulloret specifike për llojin e organizatës dhe të dhënat që organizata i trajton.
- Treshja e CIA-s përbëhet nga konfidencialiteti, integriteti dhe disponueshmëria.
- Modelet e kontrollit të qasjes bazë përfshijnë si në vijim:
 - Kontrolli i detyrueshëm i qasjes (MAC)
 - Kontrolli diskrecional i qasjes (DAC)
 - Kontrolli jo-diskrecional i qasjes
 - Kontrolli i qasjes i bazuar në attribute (ABAC)
 - Parimi i privilegjit më të vogël

Përmbledhje

- Kontrolli i qasjes AAA përfshin autentifikimin, autorizimin dhe kontabilitetin.
- Dy metoda të zakonshme të autentifikimit janë Authentication AAA Local dhe Authentication AAA Authentication.
- Kontabiliteti AAA mban një regjistër të hollësishëm të saktësisht se çka bën përdoruesi i legalizuar në pajisje.
- Regjistrat AAA të kontabilitetit përfshijnë:
 - Kontabiliteti i Rrjetit
 - Kontabiliteti i Lidhjes
 - EXEC Kontabiliteti
 - Sistemi i Kontabilitetit
 - Komandën e Kontabilitetit
 - Kontabiliteti i resurseve

Përmbledhje

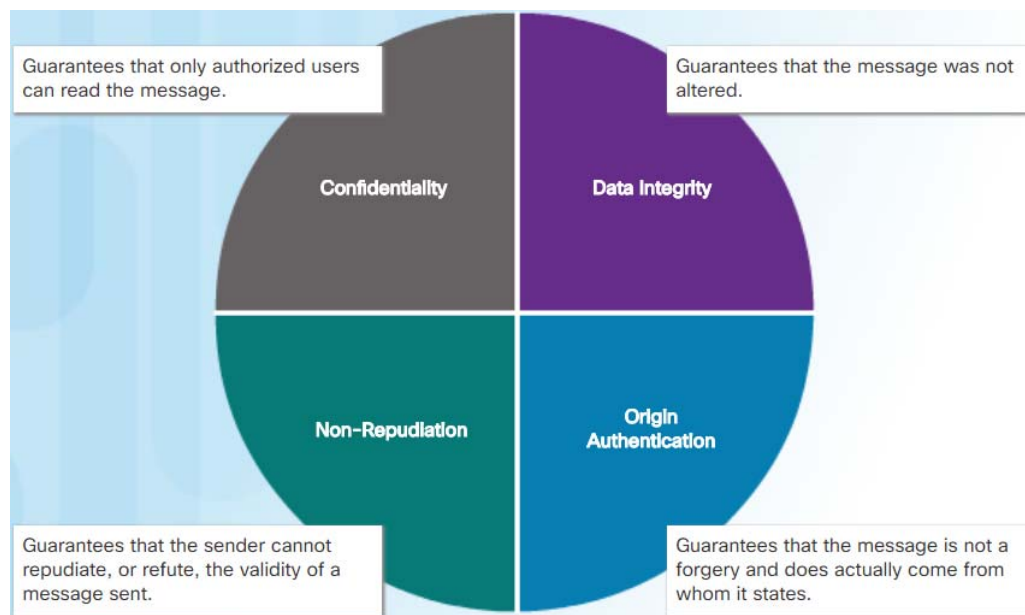
- Organizatat e inteligjencës kërcënuese si CERT, SANS dhe MITER ofrojnë informacione të hollësishme mbi kërcënimet që janë jetike për praktikën e sigurisë kibernetike.
- Raporti i Cybersecurity Cisco ofron një përditësim mbi gjendjen e sigurisë.
- Bloget dhe podcastet e sigurisë ndihmojnë profesionistët e sigurisë kibernetike të kuptojnë dhe zbusin kërcënimet në zhvillim.
- Shërbimet e inteligjencës kërcënojnë shkëmbimin e informacionit të kërcënimit.
- FireEye ofron informacion të kërcënimit në rritje dhe raporte të inteligjencës së kërcënimit.
- AIS krijon një ekosistem ku, sapo të njihet një kërcënim, ajo ndahet menjëherë me komunitetin.
- Baza e të dhënave të CVE përdor një skemë të standardizuar të emërimit për të lehtësuar ndarjen e inteligjencës së kërcënimit.
- Standardet STIX dhe TAXII lehtësojnë shkëmbimin e informacionit të kërcënimeve duke specifikuar strukturat e të dhënave dhe protokollet e komunikimit.

Kriptografia

Çfarë është kriptografia?

Sigurimi i komunikimeve

- Shqetësimet e sigurisë së informacionit që mbrojnë pajisjet e infrastrukturës së rrjetit dhe sigurimin e të dhënave gjatë udhëtimit në rrjet.
- Kriptografia ndihmon në realizimin e katër objektivave të sigurisë së informacionit:
 - **Konfidencialiteti i të dhënave** - vetëm përdoruesit e autorizuar mund t'i lexojnë të dhënat.
 - **Integriteti i të dhënave** - të dhënat nuk janë ndryshuar nga palët e paautorizuara.
 - **Authentication origjinës** - të dhënat në të vërtetë kanë origjinën në burimin e pritshëm.
 - **Mosdeklarimi** - integriteti i mesazhit është i pakundërtueshëm nga dërguesi.



Çfarë është kriptografia? Kriptologjia

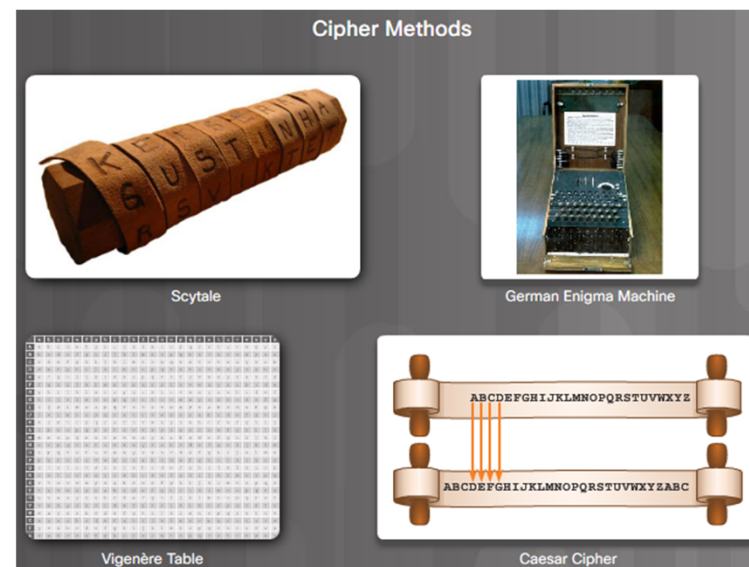
- Kriptologjia është shkenca e bërjes dhe thyerjes së kodeve sekrete. Ka dy disiplina:
 - Kriptografia - Ky është zhvillimi dhe përdorimi i kodeve që përdoren për komunikim privat. Në mënyrë të veçantë, është praktika dhe studimi i teknikave për të siguruar komunikimet.
 - Kriptoanaliza - Kjo është thyerja e kodeve. Në mënyrë të veçantë, është praktika dhe studimi i përcaktimit dhe shfrytëzimit të dobësive në teknikat kriptografike.



Çfarë është kriptografia?

Kriptografia - Shifrat

- Një shifër është një algoritëm që përbëhet nga një seri hapash të përcaktuar mirë që mund të ndiqen si një procedurë gjatë kriptimit dhe dekriptimit të mesazheve.
- Më poshtë janë llojet e shifrave që janë përdorur gjatë viteve:
 - Zëvendësimi i shifrimit - Zëvendësimi i shifrave ruan frekuencën e mesazhit origjinal.
 - Shifra e transpozimit - Në shifrat e transpozimit, asnjë letër nuk zëvendësohet; ato thjesht ndryshohen.
 - Shifrat polyalphabetic - Shifrat polyalphabetic bazohen në zëvendësimin, duke përdorur alfabetet e shumëfishta zëvendësimi.



Çfarë është kriptografia?

Kriptoanaliza - Thyerja e kodit

- Ekzistojnë një numër i metodave të thyerjes së kodit (kriptoanaliza), të tilla si forca brutale, ciphertext dhe i njohur tekst-plaintext, ndër të tjera.
- Disa metoda përdoren në kriptanalizë:
 - Brute-force - Kriptanalisti përpiqet çdo çelës të mundshëm duke e ditur se përfundimisht njëri prej tyre do të punojë.
 - Ciphertext - Kriptanalisti ka tekstin cipher të disa mesazheve të koduara, por nuk ka njohuri për tekstin themelor.
 - I njohur - Plaintext - Kriptanalisti ka qasje në tekstin cipher të disa mesazheve dhe di diçka rreth teksteve të thjeshta që qëndrojnë në themel të asaj cipë.
 - Zgjedhur-Plaintext - Kriptanalisti zgjedh të dhënat që pajisja e kodimit krijon encrypted dhe vëzhgon output ciphertext.
 - Zgjedhur-Ciphertext - Kriptanalisti mund të zgjedhë shifra të ndryshme ciprike që do të decrypted dhe ka qasje në plaintext decrypted.
 - Meet-in-the-Middle - Kriptanalisti njih një pjesë të thjeshtë dhe tekstin përkatës të ciprës.

Çfarë është kriptografia? Qelësat

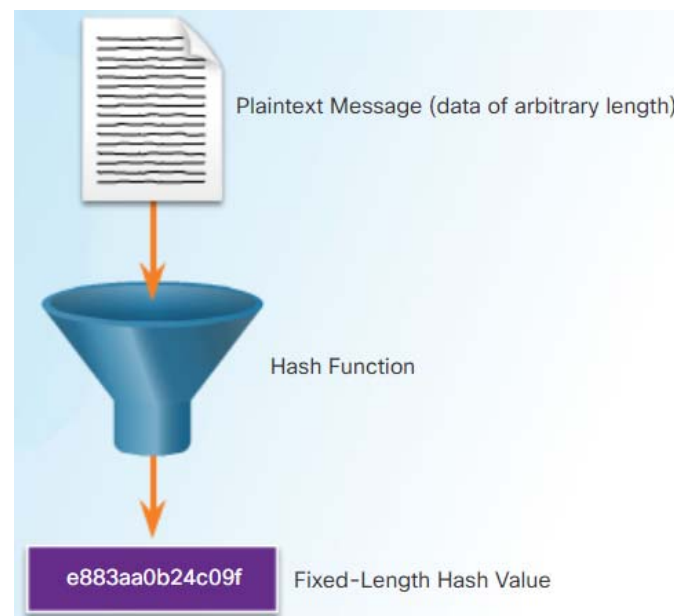
- Me teknologjinë moderne, siguria e enkriptimit qëndron në sekretin e çelësave, jo në algoritmin.
- Dy terma që përdoren për të përshkruar çelësat janë:
 - Gjatësia kryesore - E quajtur edhe madhësia kryesore, kjo matet në copa. Në këtë kurs, ne do të përdorim termin gjatësi kyçe.
 - Keyspace - Ky është numri i mundësive që mund të krijohen nga një gjatësi specifike kyçe.
- Ndërsa rritet gjatësia kryesore, hapësira e çelësave rritet në mënyrë eksponenciale.

DES Key	Keyspace	# of Possible Keys
56-bit	2^{56} 111111 111111 111111 111111 111111 111111 111111	72,000,000,000,000,000
57-bit	2^{57} 111111 111111 111111 111111 111111 111111 111111 1	144,000,000,000,000,000
58-bit	2^{58} 111111 111111 111111 111111 111111 111111 111111 11	288,000,000,000,000,000
59-bit	2^{59} 111111 111111 111111 111111 111111 111111 111111 111	576,000,000,000,000,000
60-bit	2^{60} 111111 111111 111111 111111 111111 111111 111111 1111	1,152,000,000,000,000,000

Integriteti dhe origjinaliteti

Funksionet kriptografike Hash

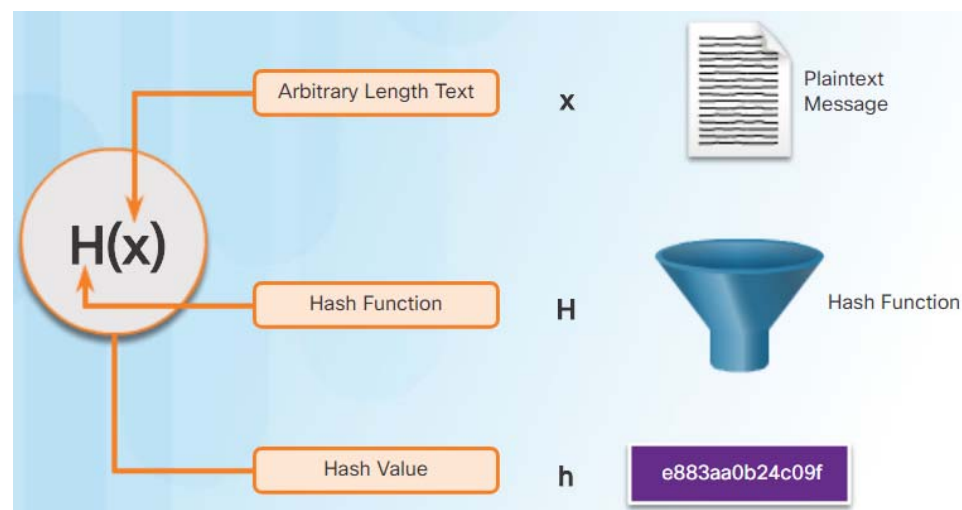
- Hierat kriptografike përdoren për të verifikuar dhe siguruar integritetin e të dhënave.
- Hashing bazohet në një funksion matematik të njëanshëm që është relativisht i lehtë për të llogaritur, por shumë më vështirë për t'u kthyer.
- Funksioni hashing kriptografik gjithashtu mund të përdoret për të verifikuar vërtetimin.
- Një funksion hash merr një bllok të ndryshueshëm të të dhënave binare, që quhet mesazhi, dhe prodhon një përfaqësim të fiksuar, të kondensuar, të quajtur hash.
- Hash-i që rezulton është gjithashtu i quajtur edhe thërrmimi, trullosja ose digjitalizimi i mesazhit.
- Me funksione hash, është computably impossible për dy grupe të ndryshme të të dhënave për të dalë me të njëjtën output hash.
- Çdo herë që të dhënat ndryshohen ose ndryshohen, vlera e hash gjithashtu ndryshon.



Integriteti dhe origjinaliteti

Operacionet kriptografike Hash

- Matematikisht, ekuacioni $h = H(x)$ përdoret për të shpjeguar se si funksionon një algoritëm hash.
- Një funksion hash kriptografik duhet të ketë vetitë e mëposhtme:
 - Hyrja mund të jetë çdo gjatësi.
 - Produkti ka një gjatësi fikse.
 - $H(x)$ është relativisht e lehtë për të llogaritur për çdo x të dhënë.
 - $H(x)$ është një mënyrë dhe jo e kthyeshme.
 - $H(x)$ është pa përplasje, që do të thotë se dy vlera të ndryshme të hyrjes do të rezultojnë në vlera të ndryshme hash.



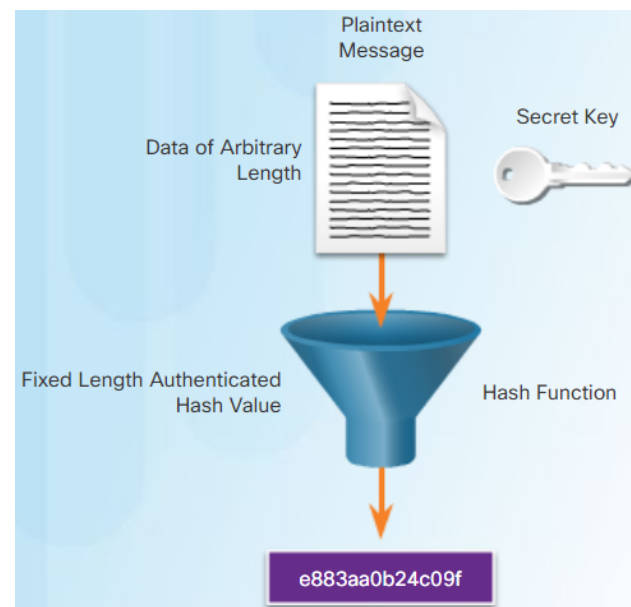
Integriteti dhe origjinaliteti MD5 dhe SHA

- Funkzionet Hash përdoren për të siguruar integritetin e një mesazhi. Ata sigurojnë që të dhënat nuk kanë ndryshuar aksidentalisht apo me dashje.
- Tre algoritme të njohura të hashing-it janë 128-bit MD5, SHA-1 dhe SHA-2.
 - MD5 me 128-bit digest - Një funksion i njëanshëm që prodhon një mesazh 128-bit hashed. MD5 konsiderohet të jetë një algoritëm trashëgimi. Rekomandohet që SHA-2 të përdoret në vend të kësaj.
 - SHA-1 - Shumë e ngjashme me funksionet hash të MD5. Ekzistojnë disa versione. SHA-1 krijon një mesazh 160 bit dhe është pak më i ngadalshëm se MD5. SHA-1 ka defekte të njohura dhe është një algoritëm trashëgimi.
 - SHA-2 - algoritmi i gjenerimit të ardhshëm dhe duhet të përdoret sa herë që të jetë e mundur.
- Ndërsa hashing mund të përdoret për të zbuluar ndryshimet aksidentale, nuk mund të përdoret për të mbrojtur kundër ndryshimeve të qëllimshme. Nuk ka asnjë informacion identifikues unik nga dërguesi në procedurën e hashingut.



Integriteti dhe origjinaliteti Kodi i Autentifikimit të Mesazhit Hash

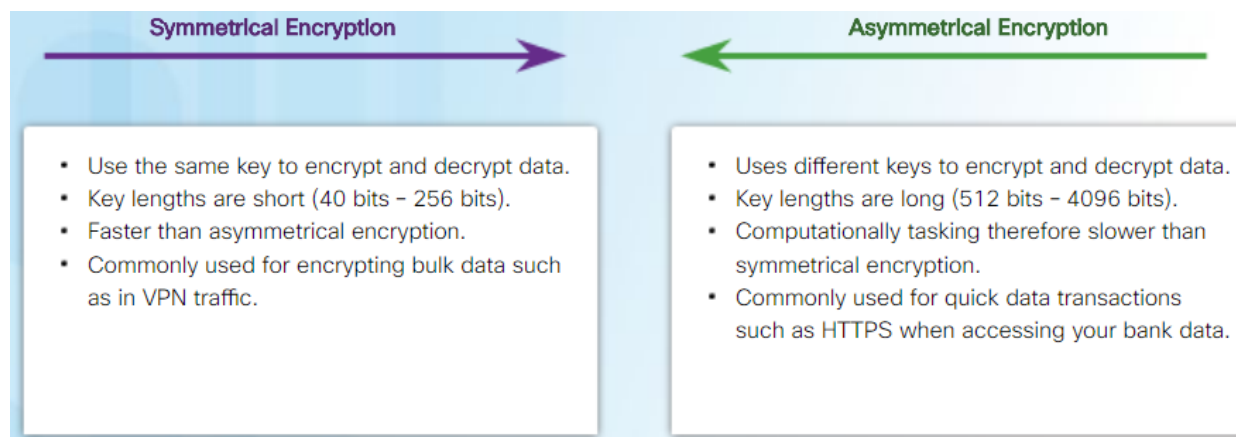
- Për të shtuar autentikimin për sigurimin e integritetit, përdoret një kod i legalizuar i mesazhit të mesazhit të hash (HMAC).
- Për të shtuar autentikimin, HMAC përdor një çelës sekret shtesë si hyrje në funksionin hash.
- Vetëm dërguesi dhe marrësi e dinë çelësin e fshehtë, dhe prodhimi i funksionit të hash-it tani varet nga të dhënat e hyrjes dhe çelësi i fshehtë.
- Vetëm partitë që kanë qasje në këtë çelës sekret mund të llogarisin thyerjen e një funksioni HMAC.
- Nëse tretet që llogaritet nga pajisja marrëse është e barabartë me tretjen që u dërgua, mesazhi nuk është ndryshuar.



Konfidencialiteti Enkriptimi

Këto dy klasa ndryshojnë në mënyrën se si përdorin çelësat:

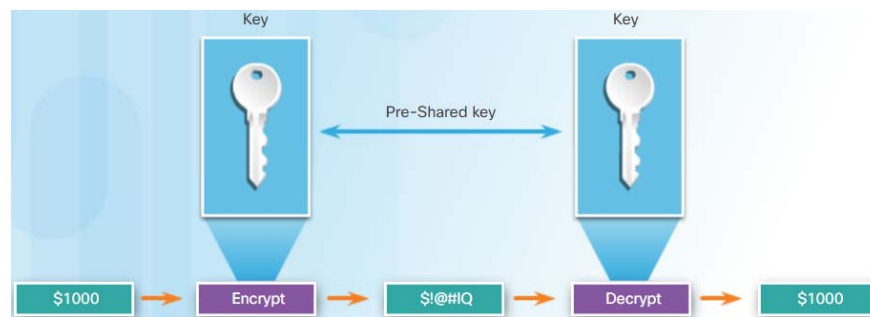
- Algoritmet simetrike të enkriptimit - Algoritmet e kodimit përdorin të njëjtin çelës për të koduar dhe dekriptuar të dhënat. Ata bazohen në premisat që secila parti komunikuese e di çelësin e paracaktuar.
- Algoritme encryption asimetrike - Algoritmet e encryption përdorin çelësa të ndryshëm për të encrypt dhe decrypt të dhënave. Ata bazohen në supozimin se dy partitë komunikuese nuk kanë ndarë më parë një sekret dhe duhet të krijojnë një metodë të sigurt për ta bërë këtë. Algoritmet asimetrike janë të burimeve intensive dhe më të ngadalshme për t'u ekzekutuar.



Konfidencialiteti

Enkriptimi simetrik

- Algoritmet simetrike përdorin të njëjtin çelës të parazgjedhur për të koduar dhe dekriptuar të dhënat.
- Sot, algoritmet simetrike të kodimit përdoren zakonisht me trafik VPN. Kjo sepse algoritmet simetrike përdorin më pak CPU sesa algoritmet e kodimit asimetrike.
- Kur përdoren algoritme simetrike të enkriptimit, si çdo lloj tjetër i enkriptimit, sa më gjatë çelësi, aq më shumë do të duhet që dikush të zbulojë çelësin.
- Shumica e çelësve të kodimit janë ndërmjet 112 dhe 256 bit. Përdorni një çelës më të gjatë për komunikime më të sigurta.

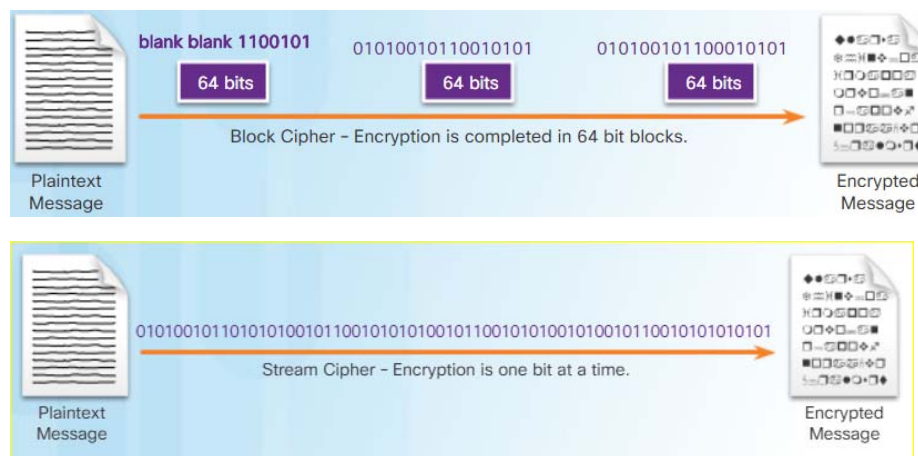


Konfidencialiteti

Algoritmet simetrike të enkriptimit

Algoritmet e encryption zakonisht klasifikohen si:

- Shifrat e bllokut - Shifrat e bllokut transformojnë një bllok të fiksuar të një teksti të thjeshtë në një bllok të zakonshëm të ciprës së 64 ose 128 bits.
- Shifrat e drejtpërdrejtë - Shifrat e transmetimit të encrypt plaintext një byte ose një bit në një kohë.

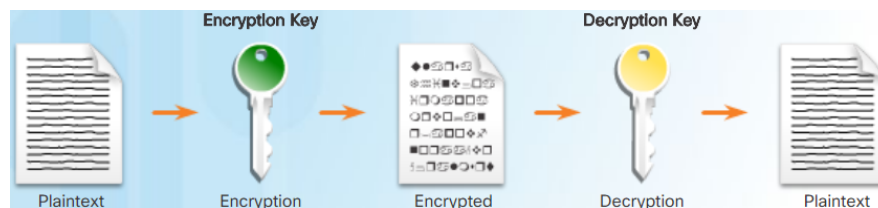


Algoritme simetrike të kodimit të njohur përfshijnë: Standard Encryption Data (DES), 3DES (Triple DES), Advanced Encryption Standard (AES) Algoritmi Encryption Optimized Software (SEAL), Shifrat Rivest (RC)

Konfidencialiteti

Algoritmet Asimetrike të Kriptimit

- Algoritmet asimetrike, të quajtura edhe algoritme me çelës publik, janë projektuar në mënyrë që çelësi që përdoret për enkriptim është i ndryshëm nga çelësi që përdoret për dekriptim.
- Çelësi i dekriptimit nuk mund të llogaritet në asnjë kohë të arsyeshme nga çelësi i kodimit dhe anasjelltas.
- Algoritmet asimetrike përdorin një çelës publik dhe një çelës privat.
- Të dy çelësat janë të aftë për procesin e enkriptimit, por çelësi plotësues i çiftëzuar kërkohet për dekriptim.
- Procesi është gjithashtu i kthyeshëm në atë të dhënash të koduara me çelësin publik që kërkon çelës privat për të dekriptuar.
- Ky proces mundëson algoritme asimetrike për të arritur konfidencialitetin, vërtetimin dhe integritetin.

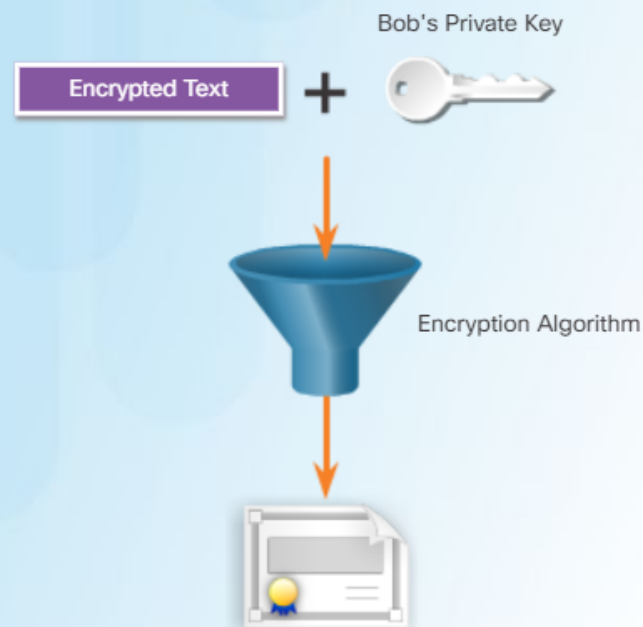


Konfidencialiteti

Enkriptimi asimetrik - Konfidencialiteti

- Algoritmet asimetrike përdoren për të siguruar konfidencialitet pa para-ndarjen e një fjalëkalimi.
- Qëllimi i konfidencialitetit të algoritmeve asimetrike fillohet kur procesi i enkriptimit fillon me çelësin publik.
- Procesi mund të përmbledhet duke përdorur formulën: Çelësi publik (Encrypt) + Çelësi privat (Decrypt) = Konfidencialiteti
 - Kur çelësi publik përdoret për të koduar të dhënat, duhet të përdoret kyç privat për të dekriptuar të dhënat.
 - Vetëm një mikse ka çelësin privat.

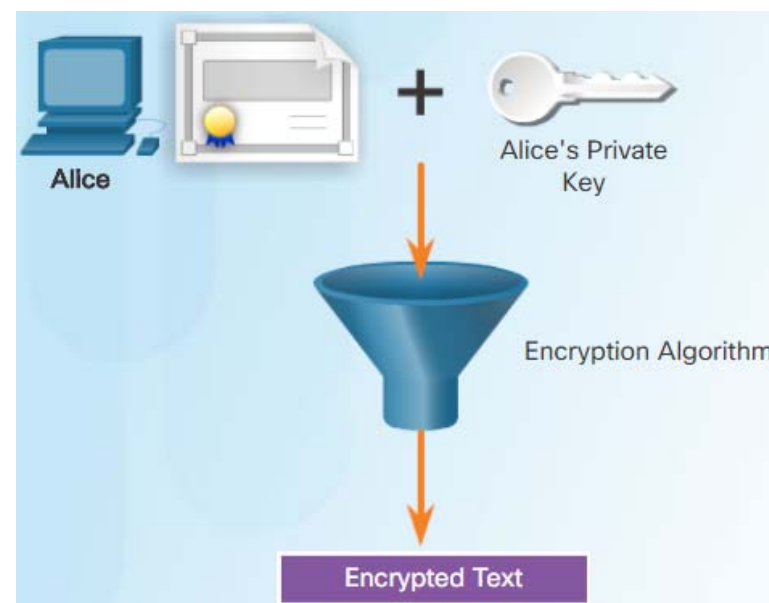
Bob Decrypts the Message Using His Private Key



Konfidencialiteti

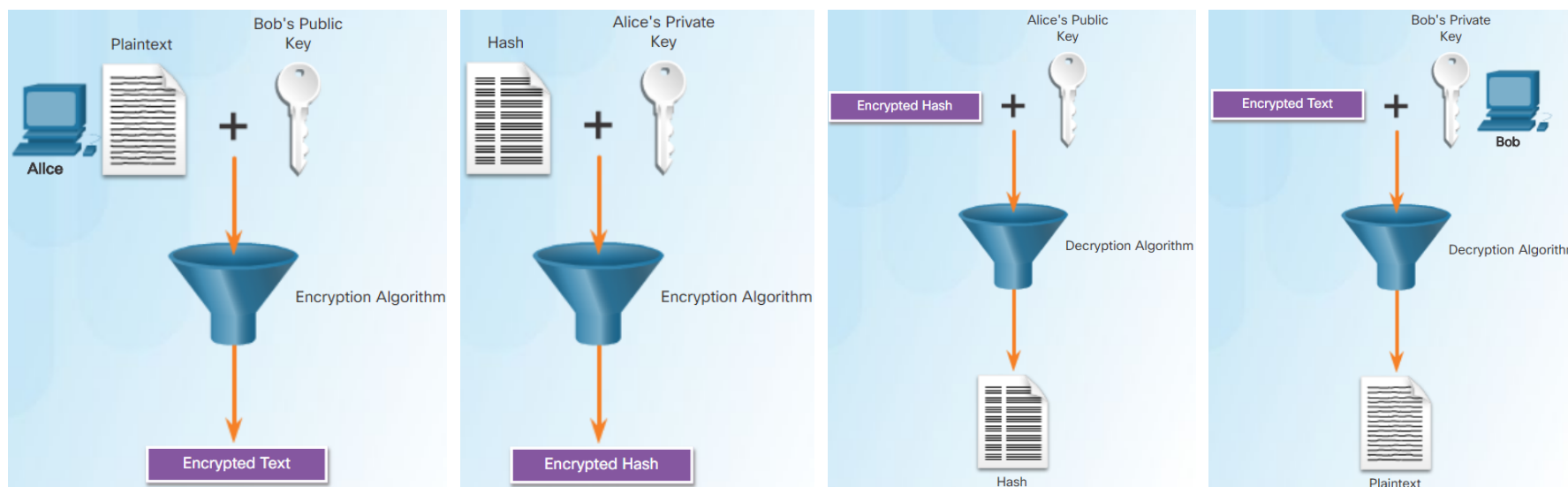
Enkriptimi asimetrik - Authentication

- Qëllimi i legalizimit të algoritmave asimetrike është iniciuar me procesin e enkriptimit të çelësit privat.
- Procesi mund të përmblihet duke përdorur formulën
- Çelësi privat (Encrypt) + Tasti publik (Decrypt) = Autentifikim
- Kur çelësi privat përdoret për të enkriptuar të dhënat, duhet të përdoret çelësi përkatës publik për të dekriptuar të dhënat.
- Për shkak se vetëm një mikpritës ka çelësin privat, vetëm ai strehë mund të ketë koduar mesazhin, duke siguruar vërtetimin e dërguesit.
- Kur një host me sukses decrypts një mesazh duke përdorur një çelës publik, ajo është e besuar se çelësi privat encrypted mesazh, i cili verifikon dërguesit.



Konfidencialiteti Enkriptimi asimetrik - Integriteti

- Kombinimi i dy proceseve të encryption asimetrike siguron konfidencialitetin, autentifikimin dhe integritetin e mesazhit.



Konfidencialiteti Diffie-Hellman

- Diffie-Hellman (DH) është një algoritëm matematik asimetrik që lejon dy kompjuterë të gjenerojnë një sekret të përbashkët identik pa komunikuar më parë.
- Kyç i ri i përbashkët nuk është shkëmbyer në të vërtetë mes dërguesit dhe pranuesit.
- Megjithatë, për shkak se të dy palët e njohin atë, çelësi mund të përdoret nga një algoritëm encryption për të encrypt trafikun midis dy sistemeve.
- Siguria e DH është e bazuar në faktin se ai përdor një numër të jashtëzakonshëm të madh në llogaritjet e tij.
- Për fat të keq, sistemet asimetrike kyçe janë jashtëzakonisht të ngadalta për çdo lloj encryption pjesa më e madhe. Kjo është arsyeja pse është e zakonshme që të enkriptohet pjesa më e madhe e trafikut duke përdorur një algoritëm simetrik.

